IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
SHERMAN DIVISION

JAMES CELESTE, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. INTRUSION, INC., JACK B. BLOUNT, MICHAEL L. PAXTON, B. FRANKLIN BYRD, P. JOE HEAD, GARY DAVIS, and JAMES GERO, Defendants.	§ CIVIL ACTION NO. 4:21-cv-00307-SDJ § [**LEAD CASE**] § § **AMENDED CLASS ACTION COMPLAINT** § **FOR VIOLATIONS OF THE FEDERAL** § **SECURITIES LAWS** § § CLASS ACTION § § § §
GEORGE NEELY and JOAN NEELY, Individually and on Behalf of All Others Similarly Situated, Plaintiff, v. INTRUSION, INC., JACK B. BLOUNT, MICHAEL L. PAXTON, B. FRANKLIN BYRD, P. JOE HEAD, GARY DAVIS, and JAMES GERO, Defendants.	§ CIVIL ACTION NO. 4:20-cv-00374-SDJ § **[CONSOLIDATED]** § § CLASS ACTION § § § § § § § § §

Lead Plaintiff Andrew Bronstein ("Plaintiff"), individually and on behalf of all others similarly situated, by and through his attorneys, alleges the following upon information and belief, except as to those allegations concerning Plaintiff, which are alleged upon personal knowledge. Plaintiff's information and belief is based upon, among other things, their counsel's investigation, which includes without limitation: (a) review and analysis of regulatory filings made by Intrusion Inc. ("Intrusion" or the "Company") with the United States ("U.S.") Securities and Exchange Commission ("SEC"); (b) review and analysis of press releases and media reports issued by and disseminated by Intrusion; (c) interviews with former employees of Intrusion; and (d) review of other publicly available information concerning Intrusion.

NATURE OF THE ACTION AND OVERVIEW

1. This is a class action on behalf of persons and entities that purchased or otherwise acquired Intrusion securities between October 14, 2020, and August 26, 2021, inclusive (the "Class Period"). Plaintiffs pursue claims against the Defendants under the Securities Exchange Act of 1934 (the "Exchange Act"). This lawsuit concerns a scheme by various officers and directors of Intrusion, Inc. to boost the price of the Company's stock by marketing a new network security product—called Intrusion Shield ("Shield")—which they represented would use proprietary artificial intelligence technology to analyze, identify, and automatically block cyberattacks, specifically including "zero-day" attacks.

2. In truth, the Company had no such artificial intelligence capability. The product they did attempt to market was slapped-together repackaging of two previously-existing Intrusion products—Savant and TraceCop.

3. Defendants rushed the project to market, from the date it was "visualized" by the then newly-hired CEO Defendant Jack Blount to a "general availability" release six months later. In the process, Defendants claimed that the Shield had identified and stopped over ***77 million***

threats to thirteen companies participating in Intrusion's beta test. This was a lie—the testing that Intrusion had conducted (such as it was) was carried out in fake test beds, not by actual customers on open networks.

4. Defendants further claimed that all but one of the beta participants signed on to pay for the product—in reality, none had. All the purported "beta" participants were existing customers or related entities—none actually signed on to pay for the service Intrusion was marketing.

5. To generate the appearance of market interest, Defendants colluded to falsely claim that they had signed two huge contracts—with consumer-products giant Kimberly Clark and components supplier Lippert Industries—to pay for Shield protection of over 50,000 seats—which, if true, would have immediately grown Intrusion's revenues by 300% or more. However, neither of those customers ever signed up to, or did, adopt Intrusion's Shield product.

6. Instead, Defendants conspired to book revenues owing from Kimberly-Clark and Lippert for legacy products and services as sales of Shield. Meanwhile, behind the scenes at Intrusion, the Company was scrambling to generate the appearance of sales, shipping out hardware and offering services free-of-charge—but the few units they were placing were failing so spectacularly that Intrusion's customer service personnel simply turned off alerts, unable to address all the errors that were flowing in.

7. The Shield product's development had been so inept, and its testing process so deficient, that the product the Company was shipping was worse than non-functional—and was, in fact, shutting down networks to which it was added, such that those testing it were forced to operate the devices in "observation mode" only.

8. Yet Defendants continued to lie to investors and to their customers and potential customers, that the Shield rollout was proceeding apace, and revenues were right around the

corner. In April 2021, an activist investor, White Diamond Research, issued a scathing report flagging some of the issues with Intrusion and its Shield project, causing a significant drop in the price of the Company's stock.

9. Instead of coming clean, however, Intrusion doubled down on its previous misstatements, issuing a purported refutation which simply compounded and added to their previous lies. The scheme only truly collapsed when the rollout of 50,000 Shield seats—and the anticipated revenues therefrom—failed to materialize.

10. The Company abruptly fired its CEO, Defendant Blount, laid off 20% of its workforce, and disclosed that it was under investigation by the U.S. Securities and Exchange Commission ("SEC").

11. As a result, the price of Intrusion's stock has utterly collapsed, from a high of over $28/share prior to the White Diamond report, to less than $4/share at the end of the Class Period—and where it sits today. Shareholders have been left holding the bag, some having lost nearly 90% of the value of their investment.

JURISDICTION AND VENUE

12. The claims asserted herein arise under Sections 10(b) and 20(a) of the Exchange Act (15 U.S.C. §§ 78j(b) and 78t(a)) and Rule 10b-5 promulgated thereunder by the SEC (17 C.F.R. § 240.10b-5).

13. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331 and Section 27 of the Exchange Act (15 U.S.C. § 78aa).

14. Venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b) and Section 27 of the Exchange Act (15 U.S.C. § 78aa(c)). Substantial acts in furtherance of the alleged fraud or the effects of the fraud have occurred in this Judicial District. Many of the acts charged herein, including the dissemination of materially false and/or misleading information,

occurred in substantial part in this Judicial District. In addition, the Company's principal executive offices are in this District.

15. In connection with the acts, transactions, and conduct alleged herein, Defendants directly and indirectly used the means and instrumentalities of interstate commerce, including the U.S. mail, interstate telephone communications, and the facilities of a national securities exchange.

PARTIES

16. Lead Plaintiff Andrew Bronstein, as set forth in the certification and associated Schedule A accompanying his previously-filed *Motion for Consolidation of Related Cases, Appointment as Lead Plaintiff and Approval of Lead Plaintiff's Selection of Counsel* (ECF #15-3 and #15-4), incorporated by reference herein, purchased Intrusion securities during the Class Period, and suffered damages as a result of the federal securities law violations and false and/or misleading statements and/or material omissions alleged herein.

17. Defendant Intrusion is incorporated under the laws of Delaware with its principal executive offices located at 101 East Park Blvd., Suite 1300, Plano, Texas 75074. Intrusion's common stock trades on the NASDAQ exchange under the symbol "INTZ."

18. Defendant Jack B. Blount ("Blount") was the Company's Chief Executive Officer ("CEO"), President and Chairman of the Board from the beginning of the Class Period until he was terminated from all roles on or about July 19, 2021.

19. Defendant Michael L. Paxton ("Michael Paxton") was the Company's Chief Financial Officer ("CFO"), Treasurer, and Secretary from August 2002 to December 31, 2020. Paxton was also a member of the Company's Board of Directors from 2019 until December 31, 2020, and Chairman of the Board from November 2019 to August 2020. He also previously served as interim President & CEO from November 2019 to May 2020. Defendant Paxton is the

son of deceased Intrusion co-founder G. Ward Paxton, Jr.

20. Defendant B. Franklin Byrd ("Byrd") was the Company's Chief Financial Officer ("CFO") from December 2020 through the end of the Class Period.

21. Defendant P. Joe Head ("Head") was the Company's co-founder and Chief Information Officer ("CIO") at all relevant times.

22. Defendant Gary Davis ("Davis") was the Company's Chief Marketing Officer ("CMO") from February 22, 2021, through the end of the Class Period.

23. Defendant James Gero ("Gero") was at all relevant times a purportedly independent Director of Intrusion.

24. Defendants Blount, Byrd, Paxton, Head, Davis, and Gero are sometimes referred to herein as the "Individual Defendants."

25. Each of the Individual Defendants:

(a) directly participated in the management of the Company;

(b) was directly involved in the day-to-day operations of the Company at the highest levels;

(c) was privy to confidential proprietary information concerning the Company and its business and operations;

(d) was directly or indirectly involved in drafting, producing, reviewing and/or disseminating the false and misleading statements and information alleged herein;

(e) was directly or indirectly involved in the oversight or implementation of the Company's internal controls;

(f) was aware of or recklessly disregarded the fact that the false and misleading statements were being issued concerning the Company; and/or

(g) approved or ratified these statements in violation of the federal securities laws.

FORMER EMPLOYEE ("FE") WITNESSES

26. FE # 1 worked for Intrusion from December 2020 through August 2021. FE #1 was hired as Director of Defense Cybersecurity and subsequently promoted to the position of Vice President of Sales for Government and Defense. FE #1 was based out of Intrusion's headquarters in Plano, Texas, and reported directly to Defendant Head, and later to Defendant Blount. FE #1 Was hired in December of 2020 specifically to help lead the launch of Intrusion's Shield product. Prior to joining Intrusion, FE #1 had over a decade of experience as an intelligence analyst and program security officer, handling security oversight and contracting compliance, in the U.S. military. FE #1 subsequently spent five years as a consultant to businesses and individuals involved in government contracting and seeking to obtain or retain security clearances. At Intrusion, FE#1's responsibilities broadly encompassed government and defense contracting—including sales, certifications, pipeline, and new lead generation. FE #1 reported on and participated in frequent meetings and discussions concerning Intrusion Shield with Defendants Blount, Head, and Davis.

27. FE #2 was Intrusion's Sales Manager for Government and Defense from December 2020 until October 2021. FE #2 was hired to and did work remotely throughout their tenure, and reported directly to FE #1, and later to Defendant Davis. FE #2's responsibilities included, primarily, business development in Intrusion's enterprise channel. Prior to joining Intrusion, FE #2 worked in cybersecurity sales and services for more than two decades. FE #2 participated in frequent meetings and conversations with Defendant Head, Defendant Davis, and VP of Engineering Blake Dumas, particularly as related to Intrusion Shield, in which sales, government certification, product testing, and customer support issues were discussed.

28. FE #3 worked as Intrusion's VP and later Senior VP ("SVP") of People and Culture from October 2020 to July 2021, and then as SVP of Operations until August 2021. FE

#3 was based out of Intrusion's Plano, Texas offices. FE #3, as VP and SVP of People and Culture, was effectively the head of Human Resources for Intrusion, reported directly to Defendant Blount, and was party to regular meetings and conversations about Intrusion's business, and particularly Intrusion Shield, with Defendants Head and Byrd.

29. FE #4 was employed by Intrusion as Director of Business Development for the western U.S. region from January 2021 to August 2021. FE #4 worked remotely throughout their tenure, and they reported directly to VP of Sales Martin Koren and later to Defendant Davis. FE #4 came to intrusion with approximately 40 years of experience as an engineer in the computer, networking, and telecommunications industry, including work as a cybersecurity consultant and system designer. FE #4 participated in discussions and meetings concerning Intrusion Shield with Intrusion senior management, including Defendant Davis.

30. FE #5 was employed as a Cyber Security Analyst at Intrusion from March 2021 to September 2021. FE #5 came to Intrusion with a background as a Cyber Security Engineer and Cyber Security Analyst, with experience in data network protocols, system and network security engineering, threat and vulnerability analysis, malware and intrusion detection and prevention, forensic network analysis, and other aspects of cybersecurity.

SUBSTANTIVE ALLEGATIONS

Background and History of Intrusion, Inc.

31. Intrusion today develops, sells, and supports products that purport to protect entities from cyberattacks by combining advanced threat intelligence with real-time artificial intelligence.

32. Intrusion offers a suite of legacy monitoring and tracking products that purport to recognize or prevent malicious and illegal activities. These include Intrusion TraceCop, which maintains databases of reported malicious IP and TCP addresses and blocks attempts to access covered networks, and Intrusion Savant, a transparent network data capture and analysis solution,

which records network activity and provides reports to the customer.

33. When Intrusion was founded in 1983 by the late G. Ward Paxton, Jr. and Defendant Head, it was with the original intent to design, manufacture, and sell secure fiber optic LAN equipment. And this is what the Company did, at first. Early in its history, Intrusion developed significant government contracting business, selling secure systems to intelligence and security agencies, principally in the U.S.[1] Members of senior management obtained security clearances, including Defendant Head, who was granted a sensitive compartmentalized information ("SCI") clearance.[2] Intrusion at one point produced a secure network switch, which it sold to U.S. intelligence agencies—including the Department of Defense ("DOD"), Central Intelligence Agency ("CIA"), and National Security Agency ("NSA").[3]

34. Members of the Company, including Defendant Head—who by all accounts was the mastermind of much of what we will relate here—began selling its secure networking products outside the U.S., including—specifically—to China and other countries to whom sales of sensitive technology was prohibited by federal regulations.[4] Upon the federal agencies' learning of Intrusion's foreign sales, Head's security clearance was revoked and the Company was blackballed, losing all of its material business with the intelligence and defense sectors.[5] Defendant Head was subsequently unable to obtain a security clearance, which prevented him from becoming CEO upon G. Ward Paxton, Jr.'s death in October 2019.[6]

35. Despite this, Intrusion maintains—in press releases, investor calls, and filings with the SEC—that the Company continues to have sensitive, intelligence-related contracts with

[1] FE #1, FE #2
[2] FE #1, FE #3
[3] FE #1, FE #2
[4] FE #1, FE #2, FE #3
[5] FE #1, FE #3
[6] FE #3

the DOD, NSA, CIA, and White House, among others.[7] According to senior personnel responsible for all government contracting during the Class Period, outside of non-sensitive business with the U.S. Navy, Intrusion has not held any significant government contracts for years prior to or during the Class Period.[8] However, because of its continuing business with the U.S. Navy, Intrusion remained a cleared defense contractor, which subjected it to export control laws that generally prohibited marketing of controlled technology outside of the U.S. absent specific dispensation from the U.S. government.[9]

36. A cadre of insiders within the Company—led by Defendant Head—engaged in a pattern of illegal conduct, selling restricted technology to foreign countries in violation of export controls and cooking the Company's books to hide the true source of its revenues, while stealing Intrusion technology and marketing it through captive entities for personal gain (a practice referred to as "sidelining").[10] Defendant Head had a pattern of shady dealings and deceit, misleading employees that he was working on classified government projects and utilizing fake company names to disguise who Intrusion's customers and vendors actually were.[11]

Intrusion Hires Defendant Jack B. Blount to Boost the Company's Stock Price in Hope of a Sale

37. The Company's founder and CEO, G. Ward Paxton, Jr., passed away in October 2019. His son, and the Company's long-time CFO, Treasurer, Secretary, and Director Michael L. Paxton, was appointed interim President, CEO, and Chairman of the Board until a new CEO could be appointed. Michael Paxton would remain in his role as CFO, Secretary, and Treasurer and Chairman of the Board of Directors until his retirement and resignation from the Board on or about December 31, 2020.

[7] FE #1
[8] FE #1
[9] FE #1
[10] FE #1, FE #2, FE #4
[11] FE #1, FE #2

38. After G. Ward Paxton, Jr.'s death, the Company's Board of Directors became interested in putting Intrusion on the market. To this end, they recruited Defendant Jack Blount as successor President and CEO on May 27, 2020. Blount marketed himself as an experienced technology executive a turnaround specialist, with a track record of helping distressed or declining companies improve and grow their business enough to sell.

39. According to Intrusion and his own public statements, Defendant Blount brought to Intrusion a lengthy history as a thought leader in the cybersecurity technology space. In a May 27, 2020, investor call, Blount told shareholders that he was personally recruited by 44th U.S. President Barack Obama to serve as Chief Information Officer at the U.S. Department of Agriculture ("USDA") between approximately 2013 and 2017. Intrusion's May 27, 2020, press release stated that Blount "served as CIO of the U.S. Department of Agriculture where he was responsible for designing a new, 10-layer cyber security architecture that protected more than 100,000 employees and billions of dollars."

40. The USDA Office of the Chief Information Officer ("OCIO") was established on August 8, 1996. The USDA's CIO from 2013 to mid-2015 was Cheryl Cook, and from mid-2015 through 2017 was Jonathan Alboum. Defendant Blount, on the other hand, appears to have been employed by the National Finance Center ("NFC"), a "certified Shared Service Provider for Human Resources Management Services" under the Office of Personnel Management ("OPM")'s Human Resources Line of Business initiative, which provides "integrated payroll and personnel systems" and "[human resources] processing services, including payroll and time & attendance (T&A) transaction processing" to various federal programs on a contract basis.

41. Defendant Blount was not seen as a visionary tech executive or business leader within the Company. "The guy was never along the lines of a technical or business [leader], but

he was a really good marketer." [12] One former employee credited Blount with the idea to market the Shield product, but characterized this as an "attempt to package crap", intentionally deceiving investors by making materially false statements about the product and purported customers that did not exist.[13]

Defendants' Scheme to Market Non-Existent "B.S." to Take Intrusion Public and Cash Out

42. Almost immediately upon being appointed CEO on May 22, 2020, Defendants Blount and Head began telling investors that Intrusion was developing a new cybersecurity product, unique and different from anything available on the market. They claimed that this new product utilized artificial intelligence to identify and stop cyberattacks in real-time, specifically including so-called "zero day" attacks—which are cyberattacks which exploit a novel computer software vulnerability which is either unknown or known and not yet mitigated.[14] In other words, Blount and Head were promising a solution, powered by artificial intelligence, which could identify and shut down an entirely novel attack vector without human intervention. Furthermore, this solution would be compatible with all existing firewalls and other in-place security layers and would be effectively "Plug and Play"—simply connect the device to a network, and it would work immediately out-of-the-box with minimal adjustment. These were spectacular claims, and predictably generated significant interest from investors. The price of Intrusion's stock rapidly began to climb.

43. On May 27, 2020, Intrusion hosted a business update call immediately following its annual meeting, led by Defendants Blount, Paxton, and Head. Head told investors that Intrusion's unnamed "new security product" was "proceeding well" toward being ready to announce. He also introduced Blount as the new President and CEO of the Company.

[12] FE #5
[13] FE #4
[14] *See generally*, Investopedia, *Zero-day Attack,* https://www.investopedia.com/terms/z/zero-day-attack.asp (last visited Feb. 7, 2022).

44. During the May 27, 2020 conference call, Blount described how, upon joining the Company, he "visualized" combining the "depth and richness of the database that this company has been using for many years" (Intrusion's existing TraceCop product) with "a product [Intrusion] had called Savant, which does real-time analysis of every packet of information going through the internet," together with "what I have been spending the last five to seven years in consulting on, which is artificial intelligence."

45. Blount continued, "When you put those three things together you can create a real-time solution that is a true defense against cyber-crime… it's not just working off a whitelist or blacklist, it's not just analyzing packets… it literally real-time stops anything that can harm you. It looks at it with AI." Blount clarified that the product Intrusion was developing would not resemble a simple firewall, noting that "every company that has been breached in the last five years had one thing in common, they all had a firewall and they got breached anyway." Instead, Blount claimed that Intrusion's new product was a "real-time device literally working in the millisecond to analyze, evaluate, and… block on the fly in coming sessions, outgoing sessions, and even internally lateral sessions."

46. Blount elaborated that the product would utilize the Company's proprietary database of "approximately 2.7 billion IP addresses… nobody in the world has a database of 2.7 billion evil IP addresses except Intrusion…" He also emphasized the importance of Intrusion's artificial intelligence, claiming, "the world has a shortage of about a million IT cybersecurity professionals… That's why we put in the AI component. AI is actually like having a team of IT engineers on your staff working 24/7…" Blount emphasized his expertise with respect to AI, in particular: "So I have been doing technology my whole life… So, I have a great appreciation for [artificial intelligence] and an understanding on how we can use it to fundamentally change the way things are done."

47. On August 24, 2020, Intrusion filed a Registration Statement on Form S-1 for a

follow-on public offering. While Intrusion's shares had previously traded over-the-counter on the OTCQB, Intrusion had applied to be up-listed to the NASDAQ under the ticker symbol, "INTZ". The Registration Statement proposed to issue 10 million new shares (beyond the then-existing 14,796,279 shares). The sole underwriter and book-running manager on the share offering was B. Riley Securities.

48. The August 24, 2020 Registration Statement discussed the Company's development of a new product, to be called Intrusion Shield:

> We are in the process of developing a new product offering, Intrusion Shield, that is designed to be a next generation intrusion detection and protection solution. After 20 years of providing research, analysis, and tools to the federal government and enterprise corporations, Intrusion possesses a comprehensive and proprietary threat enriched big data Cloud of Internet activity, including information about the activities of malicious online actors. Intrusion's Shield product will combine that comprehensive, proprietary database with artificial intelligence (AI) and real-time process flow technology to provide businesses and government agencies with a unique and affordable tool to detect, identify, and prevent cyber-crimes.
>
> Shield is a combination of plug-and-play hardware, software, global data, and AI services providing organizations with aggressive protection against unaddressed information security threats and the most robust defense possible against cybercrime. Unlike traditional industry approaches that rely heavily on human resources, which malicious actors have learned to bypass, Intrusion Shield uses our extensive threat enriched big data Cloud together with real-time AI technology to prevent illicit behavior. Shield's proprietary architecture isolates and neutralizes malicious traffic and network flows that existing solutions cannot identify or even characterize. Most breaches today are caused by malware free compromises that trigger no alarms in a firewall or endpoint solution. The common denominator is network communications, and Shield monitors and analyses all network traffic and communications allowing it to identify and stop malware-free attacks. Shield's capabilities will continuously evolve based on real-time updates originating from our worldwide installations and growing TraceCop database identifying new dangers.
>
> Shield does not require the displacement of any existing products but instead provides a new, additional layer of cybersecurity for customers. The U.S. market consists of 34 million businesses of which 70% of this market is the small and medium sized business market. While the company believes that many large enterprises will recognize the need this product addresses and will be incentivized to purchase Shield, the enterprise market has many decision makers for new security product purchases; therefore, the sale cycle may be longer for this product. We have identified businesses with from 100 to 1,000 users as our initial target market, as we believe this market segment has the most pressing need for the enhanced protection that the Intrusion

> Shield will offer. In addition to direct sales and telesales we intend to leverage existing and new channel partners, such as value added resellers and systems integrators, to market Shield to this target market.
>
> Shield has experienced positive progress during Alpha testing and we have identified twelve companies for the Beta release anticipated to begin in September. The configuration of hardware is a single Dell network appliance installed inline inside of the customer's firewall. The size of the network appliance will vary depending on the number of seats and the size of the customer's internet connection be that 1Gb, 10Gb or 100 Gb.

Defendants Pump Intrusion Shield With Falsehoods and Lies

49. A scant few months after Defendant Blount described "visualiz[ing]" this new product, on October 5, 2020, Intrusion posted a video to its public profile[15] on YouTube[16], purporting to show an "unboxing" of an Intrusion Shield hardware bridge—prominently displaying an Intrusion logo badge—and including a presentation by Defendant Head demonstrating a browser-based interface showing a "map of the world." Head represented that Intrusion possessed a "master list of good and bad domain names and host names, about 4 billion, and then we also have the master lists of all IP addresses in the world and which ones are evil and which ones are good," and then claimed that "we have a bunch of AI that adds behavioral analytics on top of that."

50. The October 5, 2020, video falsely portrayed Intrusion Shield as a complete and functioning product, when in reality, the hardware bridge shown was an off-the-shelf Dell product with Dell branding obscured and an Intrusion badge prominently affixed. Defendant Head's claim that Intrusion Shield offered artificial intelligence "behavioral analytics" was entirely false—Intrusion had no such AI technology and performed no "behavioral analytics" whatsoever. Rather, the interface Head demonstrated merely matched incoming and outgoing packets against existing, static databases and theoretically blocked (or, in "observation mode", as the device shown appears to have been operating, simply flagged) packets from known sources and hosts. The device Head

[15] YouTube, "Intrusion Shield" (Channel), https://www.youtube.com/channel/UCQSZw8FMGfJJNPMog8mHiKA (last visited Feb. 7, 2022).
[16] YouTube, "INTRUSION Shield Unboxing" (Video), https://www.youtube.com/watch?v=x-u12rzOusU (last visited Feb. 7, 2022).

showed in the video was, most charitably, a static packet-filter (or "*first-generation")* firewall—an artifact of the early 1990s. However, Defendant Head knew that the Shield program was not even capable of functioning in that capacity—Intrusion's Shield software was riddled with "show-stopping" bugs that would prohibit its use in any commercial setting in the foreseeable future. In addition, Defendants knew and failed to disclose that the Shield solution was programmed to "fail closed", blocking network activity where traffic could not be cleared—which could shut down any network to which it was attached outside of simple "observation" mode.

51. The same day the YouTube video was released, Intrusion filed an Amended Registration Statement on Form S/1A revealing participating "selling shareholders" included Defendants Head (100,000 shares), Paxton (324,432 shares), and other members of the Paxton family (in aggregate, 675,558 shares).

52. The October 5, 2020 Amended Registration Statement was largely duplicative of the August 24, 2020 version but added the following:

> Shield has received very positive feedback from Beta customers who have been surprised and pleased with the ease of installation due to the plug-n-play architecture. Within the first three days of Beta testing, **Shield identified and immediately shut down a total of 461,562 threats to three companies**, defending them against possible cyber-attacks. Customers went on to say, "It was amazing how many potential threats were blocked in such a short period of time with the Shield solution. We didn't realize how many connections were being attempted each day," said the CEO of a defense company that is participating in the Beta testing. A VP of IT at a large manufacturing company commented, "It was easy to install Shield and because of the blocking we have seen we have already installed a second Shield at a subsidiary company and we anticipate purchasing Shield when it is shipping for several of our companies."

(Emphasis added.)

53. Intrusion's claim that Shield "identified and immediately shut down a total of 461,562 threats to three companies" in the initial days of beta testing was false and misleading, as the "beta" test in question was not of customer companies on open networks, but rather based on fake test bed data.

54. On October 8, 2020, Intrusion filed a Notice of Effectiveness of the Amended Registration Statement. The following day, October 9, 2020, the company announced that its application to up-list Intrusion's shares to the NASDAQ had been approved.

55. On October 14, 2020. Intrusion issued a press release touting that it was "opening pre-orders" for its "New Cybersecurity Solution", Shield. The press release claimed that Shield took: "an entirely new approach to protecting an organization's network" and threats would be "neutralized upon detection without the traditional requirement of equipment cleansing." Intrusion further represented that it had obtained "positive results seen in the preliminary stages of beta testing, where Shield was able to stop more than 400,000 threats to three companies in just the first three days of testing." Intrusion credited this to Shield's "use of real-time AI to analyze Intrusions' threat-enriched, Big Data Cloud – the world's largest inventory of IP relationships." Intrusion reported that "using its Process-flow Technology™, the solution applies signatures and rules based on DNS, TCP, UDP – and the connections between DNS and IPV4 and IPV6 addresses – to learn the behavior and patterns of cybercrime activity. Shield then uses this intelligence while it continuously monitors incoming and outgoing traffic to identify new threats." The Company went on to claim that Shield "goes beyond monitoring by instantly stopping traffic to and from any malicious sources, protecting companies from ransomware, viruses, malware, data theft and more. Whereas other cybersecurity solutions only identify possible threats and overwhelm network managers with alerts, Shield instantly blocks these threats."

56. Intrusion's representations regarding Shield's technical capabilities and state of development were false and misleading. Far from taking "an entirely new approach", the Shield system was little more than a packet-filter firewall with a browser-based user interface, as described above. Intrusion falsely represented that Shield had achieved positive results in testing, including that it was able to "stop more than 400,000 threats" in the first three days. In truth, Intrusion falsified

these results by using a fake test bed, and the device could operate only in "observation" mode—thus, it would merely flag, rather than "stop" any suspicious packets. Intrusion's principal selling point for Shield—its AI capabilities—did not actually exist, as Shield was in no way capable of "learn[ing] the behavior and patterns of cybercrime activity" to "instantly stop[]" malicious traffic. Shield did not "go[] beyond simple monitoring" at all—in fact, as Defendants well knew, that was all the product could do.

57. On October 15, 2020, Intrusion issued a press release announcing the completion of its follow-on public offering of 3,565,000 shares at a price to the public of $8.00/share. Intrusion stated that it intended "use the proceeds to fund several growth initiatives, including the commercialization of its new Shield plug-n-play, real-time artificial intelligence (AI), threat detection and neutralization solution designed for the enterprise market."

58. On October 16, 2020, Intrusion posted a video to YouTube[17] through BusinessWire, in which Defendant Head claimed that Intrusion Shield would, "revolutionize the industry, because it shows you things you never knew that you could see and stops them without your having to look." Defendant Blount went on to say that "we have this unique database, called TraceCop, that we've been building for 25 years. We know the reality is there's 2.7 billion IP addresses that should be on that blocklist. No other product on the market could even store 2.7 billion IP addresses." Blount continued by claiming that Intrusion possessed artificial intelligence which, in conjunction with the proprietary TraceCop database, was able to "spot the bad guy", and Head explained that their artificial intelligence platform "would only have to make the decision once, and then it applies to the whole world," thus claiming that Intrusion's artificial intelligence was capable of machine learning. Blount went on to assure that, "this product isn't let's look at logs next week or next month and figure out what went wrong and how to find it, we stop it real-time."

[17] YouTube, "INTRUSION's New Cybersecurity Solution, Shield, Brings Government-Level Cybersecurity to Businesses", https://www.youtube.com/watch?v=auRONsNdtiI (last visited Feb. 7, 2022).

59. Defendants Head and Blount's statements in the October 16, 2020, video were patently false and misleading, as they knew that Shield lacked these artificial intelligence capabilities and was not, in fact, capable of learning, identifying, or generating new global rules to stop novel threats in "real-time."

60. On January 13, 2021, the Company issued a press release entitled "INTRUSION Successfully Completes Beta Testing of its Newest Cybersecurity Solution, Shield; Announces General Availability." It stated, in relevant part:

> ***Beta testing of INTRUSION Shield confirmed the solution's efficacy by stopping a total of 77,539,801 cyberthreats from 805,110 uniquely malicious entities attempting to breach 13 companies that participated in the 90-day beta program.*** Shield was able to continuously protect these companies from ransomware, denial of service attacks, malware, data theft, phishing and more. In fact, analysis by INTRUSION also concluded that Shield would have defended against the Sunburst malware that was at the heart of the recent cyberattacks involving SolarWinds and FireEye, which impacted many government agencies and 18,000 SolarWinds customers.
>
> "With the high-risk patterns we've incorporated into the rule set that feeds our AI, along with the reputation and suspicious activity that it searches for while monitoring all traffic in and out of a network, we can confidently say Shield would have protected our customers where clearly other security approaches failed," said Jack B. Blount, President and CEO of INTRUSION. "The malware had been living on the SolarWinds network for at least nine months undetected – it got past firewalls and many other cybersecurity products. This is all the more reason companies need a multi-layered approach to cybersecurity, and specifically one that stops threats in real-time to protect them from the damage cybercriminals can cause over time."
>
> ***All companies participating in the beta program have made the decision to move forward with Shield in production.***
>
> "The Shield solution has shown us that virtually every network is already infected, and front-end protection is not possible. The understanding that networks are already compromised and that the only means of protection is to monitor and restrict outgoing traffic is the breakthrough of the Shield philosophy," said Richard, President of NovaTech.
>
> Additionally, false positive security alerts – where legitimate traffic is identified as a threat – are a significant problem among cybersecurity solutions available today, with Ponemon Institute reporting that most cybersecurity companies see mistaken alerts happening 33% of the time. Cybersecurity professionals spend hundreds of

> hours investigating these alerts only to determine ultimately that there was no threat. ***Beta testing for Shield showed a median false positive rate of 0.001% of all traffic, far surpassing other solutions on the market and allowing businesses to run uninterrupted.*** Multiple beta customers were happy to report they saw zero false positives using Shield.

61. Intrusion's claim in its January 13, 2021 Press Release that Shield had "stop[ped] a total of ***77,539,801 cyberthreats from 805,110 uniquely malicious entities"*** in testing was a complete fabrication. According to former employee witnesses, including a cyber security analyst who performed hands-on work with Shield at the time, these were "imaginary numbers from the marketing team," without any basis in reality.[18] In fact, Intrusion's testing of the product, such as it was, "lacked rigor" and was based on "fake test bed data", and its claims about Shield's efficacy in testing were "wildly overstated."[19]

62. That same day, Defendants Byrd and Blount virtually hosted Intrusion's January 2021 Investor Presentation slideshow[20] touting the positive results of its beta testing of Shield. The slides claimed that Intrusion TraceCop "monetized over 25 years as a network forensics tool for federal customers" and was the "world's only database of 25 years of Internet traffic and specifically cybercrime," which Intrusion "constantly expands … with dozens of international data feeds." The Company also stated that Intrusion Savant offered "real-time process flow analysis" through a "patented network appliance designed to carry out bidirectional protocol decoding in RAM… Patented packet file systems for recording at line rates… [and] Patented, concise summaries for mass-enrichment, analysis and indefinite storage." Byrd and Blount presented that Intrusion Shield was a "new paradigm for cybersecurity" that would leverage TraceCop and Savant in "expanded new solutions for the enterprise" by applying artificial intelligence to TraceCop datasets and the Savant

[18] FE #5
[19] FE #1, FE #3
[20] This presentation was posted to Intrusion's website at https://ir.intrusion.com/events-and-presentations/event-details/2021/-Needham-Virtual-Growth-Conference/default.aspx. The presentation was made available publicly at https://wsw.com/webcast/needham103/intz/2283678 (last visited Feb. 7, 2022). The Company has subsequently deleted the associated page from its website, and the webcast of the presentation is no longer available.

sensor to "Identif[y] and kill[] all malicious traffic in **real-time.**" (Emphasis in original). Byrd and Blount continued that Intrusion Shield offered "patented technology" which "layer[ed] AI on top of TraceCop and Savant, enabling real-time killing of malicious traffic." Byrd and Blount assured that Shield would be compatible with existing firewalls and network security architecture, "positioned as a new network security layer" with "no change management" and "Plug-n-Play technology", offering "daily system updates" subject to "multiple provisional patents" already filed.

63. The statements from Defendants Byrd and Blount in the January 2021 Investor Presentation were likewise false and misleading, and for similar reasons. The "positive test results" referred to were, in fact, falsified. Shield did not, in fact, perform "real-time process flow analysis" and the "patented network appliance" was an off-the-shelf solution manufactured (and presumably "patented") by Dell, not Intrusion. Further, Byrd and Blount's claims that Shield operated as a "new network security layer" with "no change management" were unfounded and without any rational basis when the claims were made. Finally, Intrusion did not hold "multiple provisional patents" with respect to the Shield technology. This claim was a fabrication.

64. Intrusion's January 2021 Investor Presentation slideshow included purported testimonials from three "beta customers" who "comment[ed] on their experience" with Shield: B. Riley Financial, NovaTech, and Bard Associates. Intrusion's presentation did not disclose that B. Riley Financial was Intrusion's investment banker who organized its follow-on public offering in October 2020 and issued a highly positive initiation report on the stock. They also did not disclose that Bard Associates was a current Intrusion shareholder. Additionally, NovaTech was related to Intrusion through Intrusion's then Director of Security Solutions, who was a former IT Director of NovaTech and was then serving as a consultant to NovaTech on an ongoing basis.

65. On February 25, 2021, Intrusion announced its fourth quarter and full year

financial results in a press release that stated, in relevant part:

> "Since releasing INTRUSION's revolutionary Shield solution only 6 weeks ago, we have received an unprecedented amount of interest and a growing pipeline of customers that is nothing short of extraordinary," said Jack B. Blount, President and CEO of INTRUSION. "Shield is the first platform that uses real-time artificial intelligence to not just block intruders, but to kill cyberattacks including zero-days"

66. The February 25, 2021, Press Release repeated and reiterated the false claim that Shield used "real-time artificial intelligence", and further falsely claimed that Shield was able to "kill cyberattacks including zero-days." In truth, Shield lacked any functional artificial intelligence capable of process analysis or identifying novel "zero-day" cyberattacks. According to a former Intrusion cyber security analyst who worked on the product, "the claim that the Company's technology prevents zero-day attacks is not based on reality."[21] The witness related that this claim was based upon a *single incident* in which traffic related to an attack was flagged because a line of malicious code happened to have been re-used from another preceding attack—thus, the attack was identified by pure "luck", and not due to any AI capabilities of Shield.[22]

67. Intrusion hosted an earnings call for the fourth quarter of its 2020 fiscal year (the 4Q20 Earnings Call") on February 28, 2021 (approximately eight weeks into its first quarter of FY 2021), in which Defendant Blount claimed that "90% of [] beta customers" for the Shield product had become paying subscribers for the service.

68. Defendant Blount's claim that 90% of the participating companies in Intrusion's beta test had "become paying subscribers" for Shield was a complete fabrication. Literally *none* of the beta participants had paid anything for Shield or committed to use or pay for the service. Rather, all the "beta customers" for Shield were related parties of Intrusion or its officers or members of its Board of Directors, and/or were existing customers of Intrusion's legacy products and services. Notably, Blount made this claim in response to a question from analyst Zachary

[21] FE #5
[22] FE #5

Cummins of B. Riley Securities, Inc. Notably, B. Riley Financial was named as one of three "preliminary beta results" participants whose positive comments were touted in Intrusion's January 2021 Investor Relations presentation. B. Riley Financial was also Intrusion's principal investment bank and advised it in connection with its security offerings during the Class Period.

69. On March 9, 2021, Intrusion filed its annual report on Form 10-K for the period ended December 31, 2020 (the "2020 10-K") with the SEC, affirming the previously reported financial results. With respect to Intrusion Shield, the 10-K stated:

> **INTRUSION *Shield*,** our cornerstone cybersecurity solution is a comprehensive, real-time AI-based Security-as-a-Service that inspects and kills all dangerous network connections before they can do damage. What makes our approach unique is that it inspects every packet of inbound and outbound traffic and analyzes the reputation of the IP addresses (source and destination), the domain and ports it is communicating on, along with many other fields in the packet to neutralize malicious connections.
>
> Most breaches today are caused by malware free compromises that trigger no alarms in a firewall or endpoint solution. The common denominator is network , which ***Shield*** monitors and analyses, allowing ***Shield*** to identify and stop all attacks, even malware-free attacks. ***Shield****'s* capabilities continuously evolve based on constant machine learning and neural networking technology. Unlike traditional industry approaches that rely heavily on human mitigation and defensive approaches, which malicious actors and nation states have learned to bypass. ***Shield****'s* proprietary architecture isolates and neutralizes malicious traffic and network flows that existing solutions cannot identify before they harm a corporation or government organization. ***Shield*** is designed as a next generation Network Detection and Response solution.
>
> After 30 years of providing research, analysis, tools and services to the federal government and enterprise corporations, Intrusion possesses a comprehensive and proprietary data set of petabytes of Internet traffic, including information about the activities of malicious online actors. ***Shield*** integrates this rich ***TraceCop*** data set with artificial intelligence (AI) and ***Savant*** real-time process flow technology to provide our customers with a unique and affordable tool to detect, identify, and neutralize cyberattacks. In particular, the ***Shield*** AI has been specifically trained to identify and stop Zero-Day attacks and ransomware, the most prolific and crippling forms of malware today.

In its risk disclosure concerning Shield, the Company stated, in relevant part:

> ***We could experience damage to our reputation in the cybersecurity industry in the event that our Shield solution fails to meet our customers' needs or to***

> ***achieve market acceptance.*** Our reputation in the industry as a provider of entity identification, data mining, and advanced persistent threat detection solutions may be harmed, perhaps significantly, in the event that Shield fails to perform as we expect it to. If Shield does not perform as we expect, if we experience delivery delays, or if our customers do not perceive the benefits of purchasing and using Shield as part of their comprehensive cybersecurity solution, our position as a leader in this technology space may be damaged and could affect the willingness of our customers, as well as potential customers, to purchase our other solutions that function separately from Shield. Any reputational damage could result in a decrease in orders for all of our solutions, the loss of current customers, and a decrease in our overall revenues which could in turn have a material adverse effect on our results of operation.

70. Intrusion's statements in its 2020 10-K were false and misleading. As discussed in detail above, Shield was not able to "inspect[] and kill[] all dangerous network connections before they do damage", did not offer "constant machine learning and neural networking technology", and had not been and could not be "specifically trained to identify and stop Zero-Day attacks and ransomware." Intrusion Shield did not offer AI technology capable of meeting any of these claims. Further, the Company's risk disclosure concerning Shield was woefully inadequate and materially misleading in that it omitted and failed to relate that (a) Intrusion knew that its representations concerning Shield*'s* AI capabilities were false, or at least substantially misstated; (b) Intrusion knew that the Shield software was riddled with bugs and not prepared for commercial distribution, and the Company had no timeline or plan in place to correct the defects; (c) Intrusion's claims for Shield performance in testing were based on fake test bed data and were not rigorous or reliable indicators of product capabilities; and (d) in light of the foregoing, Intrusion knew or had information sufficient to conclude that the Company would, in fact, expect to encounter "delivery delays" and that release of the product to customers in its existing state would be expected to cause "reputational damage" to Intrusion and prevent customers from "perceive[ing] the benefits of purchasing and using Shield." The Company's risk disclosure was therefore materially incomplete and misleading.

71. On March 31, 2021, Intrusion issued a press release through Globe Newswire

announcing that it had "signed a new agreement which leading global consumer products company, Kimberly-Clark, to protect its network using Intrusion Shield." The press release included a purported quote from JR Schroeder, Cyber Defense Officer at Kimberly-Clark, saying "We chose Shield because we needed a solution that could simply and quickly protect our enterprise infrastructure as we continued to scale our business. Shield's ability to plug directly into our network and quickly add value without raising countless alerts will have a huge impact." It went on to trumpet Kimberly-Clark's "several global networks supporting a large manufacturing footprint as well as its 46,000 employees around the world." Defendant Blount was quoted as well, saying: "Kimberly-Clark is a great example of how multi-national corporations require a new way to protect their critical information. By integrating our best-in-class solution into their network in a matter of minutes, we provide Kimberly-Clark with a simpler, optimal means to automate network security at scale and afford them a level of protection that safeguards them against constantly evolving threats. We couldn't be more excited about having Kimberly-Clark as a Shield customer."

72. The Company's March 31, 2021, Press Release falsely claimed that Intrusion had secured a contract for Kimberly-Clark to adopt and pay for Intrusion's Shield technology, when in fact no such agreement existed or was expected. Defendants Blount and Head had negotiated with a personal contact at Kimberly-Clark to permit them to represent that they had signed Kimberly-Clark as a Shield customer to create a false impression of industry adoption and generate investor and customer interest in Intrusion and Shield. Kimberly-Clark was a customer of Intrusion legacy products and services, but never agreed to pay or paid to subscribe to Shield. Blount and/or Head fraudulently book revenues from Kimberly-Clark for legacy business as revenue derived from sales of Shield. In truth, Kimberly-Clark's existing, robust network security infrastructure was incompatible with Shield.

73. On April 6, 2021, the Company issued another press release announcing that it had signed Lippert Components, Inc. ("Lippert") "as a new INTRUSION Shield customer". It read, in relevant part:

> INTRUSION, Inc. (NASDAQ: INTZ), a leading provider of cyber-attack prevention solutions including Zero-Days, announced today that global components manufacturing giant Lippert Components (Lippert) has signed an agreement to protect its network using INTRUSION Shield. … They chose Shield for several reasons, including its use of real-time Artificial Intelligence (AI) to stop cyberattacks with 99.999 percent efficiency. In addition to using Shield to protect its own networks, Lippert will work with its supply chain to embrace Shield to ensure high availability of critical components as they continue to scale its global operations." The press release also included an endorsement, attributed to Jamie A. Schnur, Group President-Aftermarket at Lippert, saying: "We chose Shield because we needed a solution that leveraged AI to stop increasingly sophisticated cyberattacks targeting our company. We were impressed with Shield's use of rich historical threat intelligence to make decisions in real-time to determine if traffic going into and out of our network was good or bad and take immediate action."

74. The Company's April 6, 2021, Press Release concerning signing Lippert was similarly fraudulent. Like Kimberly-Clark, Lippert had not signed any agreement to purchase or pay for Shield devices or service. Lippert, too, was a past customer of legacy services from Intrusion, and a member of Intrusion's Board of Directors, Defendant James F. Gero—who was closely tied to Head, and also a long-time Director and former Chairman of Lippert and its corporate parent, LCI Industries—negotiated with Lippert to claim that it had been signed as a Shield customer. Lippert never paid for or agreed to subscribe to Shield, only receiving Shield equipment free-of-charge for testing purposes, if at all.

75. On April 13, 2021, the Company issued a press release entitled "Intrusion Q1 2021 Results Surpass Expectations." Therein, Intrusion stated, in relevant part:

> Highlights from the quarter include:
>
> - INTRUSION Shield is now protecting over 50,000 seats (almost 8x the company's original Q1 goal)
>
> - Hired new Chief Sales Officer, Darryl Athans, to drive continued growth

- Signed over 30 channel partners including resellers in Australia and Mexico

- Company now able to sell latest innovation, Shield, globally

> Since announcing the general availability of Shield in January 2021, the company wasted no time ramping up its go-to-market activities to finish the first quarter with several key wins. INTRUSION recently announced manufacturing giants Kimberly-Clark and Lippert Components signing on as Shield customers, with other customer additions including KBI and Geocent adopting Shield to protect their networks.

76. Intrusion's April 13, 2021, press release falsely claimed that Shield was "now protecting over 50,000 seats". In fact, Shield was generating no material revenue whatsoever. The "50,000 seats" claims appear to have been based on the estimate of seats if both Kimberly-Clark and Lippert had adopted Shield on a global basis. But, as detailed above, neither had done so. This claim was a fabrication to falsely suggest that Shield would generate material revenue in the present or near future. 50,000 seats, at the prices Intrusion was quoting in representations to investors ($20 to $40 per seat, per month) would be expected to generate subscription income of $1 million to $2 million, per month—or $12-24 million annually—against Intrusion's total FY 2020 revenue of $6.6 million. This thus created the false (and entirely fraudulent) impression that Intrusion's quarterly revenues would triple (or more) in the following periods.

White Diamond Research Begins to Reveal the Truth About Intrusion Shield

77. On April 14, 2021, White Diamond Research published a report alleging, among other things, that Intrusion's product, Shield, "has no patents, certifications, or insurance, which are all essential for selling cybersecurity products" and that "Shield is based on open-source data already available to the public." Thus, the report stated that "Shield is a repackaging of pre-existing technology rather than an innovative offering." Specifically, it stated:

> Despite heavy promotion and a supposedly successful beta test, we do not believe Shield represents a novel offering from INTZ. In fact, we believe the company itself has said this. During INTZ's Q420 Earnings Call, and in a buzz-word flurry (AI, cyber-, supercomputer, etc.), Blount revealed that Shield is simply a mashup

of INTZ's existing products. In Blount's words:

> Shield is really all 3 of Intrusion's technologies married together in a single product solution.

While this may initially sound exciting, it hardly represents any ground-breaking innovation.

Here are a few other statements that Blount made in the Q420 Earnings Call suggesting Shield is a repackaging of pre-existing technology rather than an innovative offering:

- "The TraceCop database that we have created, managed, grown, used for 25 years, is the core of what makes Shield work today."

- "The Savant technology that we've had and improved for 12 years, again, is a core piece of the technology of Shield. How we open, inspect every packet of data is with the Savant technology. The only new thing that there is in Shield is the artificial intelligence that learns from the database, that can interpret what it finds when it opens a packet of data, and how it can decide if it's good or bad, when humans could look at that packet of data and have not a clue whether it was normal traffic or not normal traffic."
- "You have to think about Shield as the combination of 25 years of R&D, 25 years of product and development, 25 years of expertise around cybercrime, combined into a single product."

* * *

We believe the timeline of the announcement coupled with the lack of direct R&D investment into Shield preceding Blount's appointment as CEO casts doubt on Shield as the culmination of a quarter-century master plan.

- Though INTZ's R&D accounts for ~39% of the company's expenses (aside from a small peak in 2015/2016), R&D has remained reasonably proportional to its total operating expenses.

- According to its accounting policies, INTZ expenses R&D as it is incurred, thus the recent uptick in R&D expense in 2020 would not be related to Shield (if it truly is a product launching on the back of years worth of R&D).

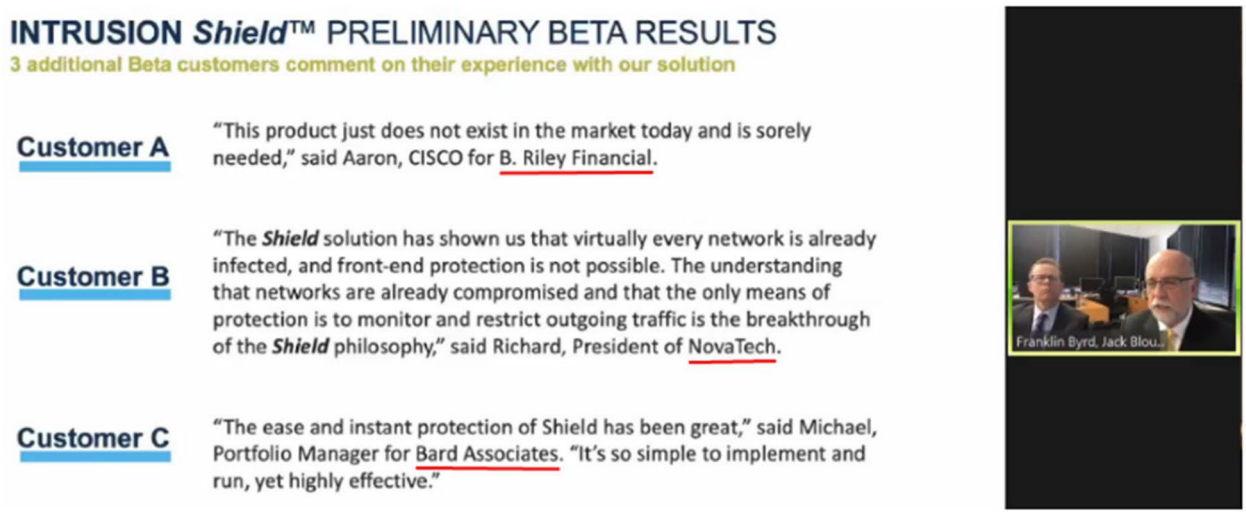
- Recent financial statements provide no indication that INTZ has been ramping up to commercialize a cutting-edge cybersecurity product.

78. Moreover, the report alleged that Intrusion's claims that Shield "stop[ped] a total of 77,539,801 cyberthreats from 805,110 uniquely malicious entities . . . in the 90-day beta program" were "outlandish," leading White Diamond to question "[h]ow have these companies

been able to function so far, as they've been attacked many times per minute by ransomware, malware, data theft, phishing and DDoS attacks?" Specifically, the report stated:

The Companies Featured From the Shield Beta Test Are Small And Have Existing Relationships with Intrusion

In INTZ's Needham Virtual Growth Conference presentation on 1/13/21, a slide shows the testimonials of three companies that were part of the Shield beta test. This slide is shown below:



* * *

All three customers have existing relationships with INTZ.

- B. Riley Financial is INTZ's investment banker who organized the equity raise in October 2020 and then issued a glowing initiation report on the stock.

- Bard Associates is a shareholder of INTZ.

- We interviewed the IT Manager for NovaTech, and he said the only reason why they got involved in the beta testing is because an IT securities guy works for both NovaTech and INTZ. We provide more details on this interview later in this section.

In the PR, INTZ made a lot of bold claims for a product with no real traction in the market. It states:

"Beta testing of INTRUSION Shield confirmed the solution's efficacy by stopping a total of 77,539,801 cyberthreats from 805,110 uniquely malicious

entities attempting to breach 13 companies that participated in the 90-day beta program. Shield was able to continuously protect these companies from ransomware, denial of service attacks, malware, data theft, phishing and more."

These numbers don't seem real, but something out of a science fiction movie. This means that on average, over the 13 companies, each company was attacked 6M times over the 90-day trial period / 66k times per day / 2.7k per hour / 46 times per minute.

[table omitted]

How have these companies been able to function so far, as they've been attacked many times per minute by ransomware, malware, data theft, phishing and DDoS attacks?

The company also claims that Shield is so good, it could have prevented the recent Sunburst malware attack. The PR states:

"In fact, analysis by INTRUSION also concluded that Shield would have defended against the Sunburst malware that was at the heart of the recent cyberattacks involving SolarWinds and FireEye, which impacted many government agencies and 18,000 SolarWinds customers."

SolarWinds (SWI) is a $5B+ IT infrastructure management software company. It sells security and data protection products. It spent $32M in Research & Development (R&D) and $82M in Sales and Marketing (S&M) in Q420, and a whopping $126M for the entire year 2020. We don't believe that INTZ has developed a more sophisticated malware defending software than SWI, given what each company has accomplished and that INTZ has invested so little in R&D.

79. White Diamond also expressed doubt that Intrusion's recent purported sales agreements would lead to significant revenue. The report stated:

On 3/31/21, INTZ announced that it signed a "new agreement" with leading global consumer products company Kimberly-Clark (KMB). One of the reasons why investors should be skeptical of this "agreement" is that the announcement doesn't include any financial details or terms on duration. We are not convinced that the contract is revenue generating and believe the "generalizations" in the announcements could imply a pilot program.

We don't believe a company the size of KMB would agree to migrate its network to a cybersecurity software that doesn't have any 3rd party certifications, without first testing it on a trial basis.

On 4/6/21, INTZ announced a new Shield customer, Lippert Components from LCI Industries (LCII). We don't think this sale is a big deal because Lippert was a former customer using INTZ's Savant service. This is also another associated

> party sale. James Gero is on the Board of Directors of both Lippert and INTZ. As shown in the screen shots below:
>
> [images omitted]
>
> Notice the Lippert executive, Jamie A. Schnur, president of the aftermarket, used the buzzword "AI" when describing why it is a Shield customer. However, Schnur isn't the IT guy in charge of cybersecurity.
>
> We spoke with the investor relations rep of LCII. He said that the CFO told him that there's a wide range of programs they use for cybersecurity. From emails, to cell phones, to any of their machinery that's hooked up to the internet. And they report to their audit committee about their cybersecurity measures.

80. In response to the White Diamond Report, on April 14, 2021, Intrusion issued a press release stating that the Company "intend[ed] to respond fully to unfounded claims made" in the White Diamond Report, and that CEO Jack Blount said that, "A short report includes claims that are blatantly inaccurate and reflect a malicious short-selling agenda. The Company is evaluating further actions."

81. On this news, the Company's share price fell $4.50, or over 16%, to close a $23.75 per share on April 14, 2021, on unusually heavy trading volume. The share pricecontinued to decline by $3.22, or 14%, over the next trading session to close at $20.53 per share on April 15, 2021.

Intrusion Denies the White Diamond Report and Doubles Down

82. In a subsequent press release on April 22, 2021, Intrusion claimed to "provide information refuting negative claims in [the] recently published short report." The Company claimed that contrary to the allegations in the White Diamond report:

- **INTRUSION** ***Shield*** is protected by two patents on existing technology: *8,291,058* and *8,472,449*. In addition, the Company filed additional patents for ***Shield*** on August 20, 2020 which are currently pending.
- The ***Shield*** application – including the logic for ***Shield'***s high-speed packet capture; connection reassembly; traffic decoding and analysis; patented packet file system; patented accumulators for performance; and kill logic – is proprietary **INTRUSION**-developed software containing over 1.1 million

lines of code. The ***Shield*** application runs on a standard server hardware platform. The platform is based on certain open-source technologies such as the Linux operating system and uses open-source databases and libraries for data storage and secure communication layers, which is very common in security appliances.

- ***Shield*** is separate and distinct from its **INTRUSION** ***TraceCop*** offering. ***Shield*** leverages the ***TraceCop*** database to train ***Shield's*** AI engine and drive its accuracy.
- ***Shield*** is in the early stage of its customer rollout and various companies, including Kimberly-Clark, Lippert Components, NovaTech, and others have entered into multi-year agreements for ***Shield***.
- **INTRUSION** has the required certifications to ship ***Shield*** to every jurisdiction where it is being sold.
- ***Shield*** is categorized as a Network Defense and Response (NDR) product designed to kill malicious connections on a network as opposed to creating alerts about suspicious traffic that tend to overwhelm IT departments and provide notifications often after damage is done to a company's network and data.

83. Intrusion's claims in its April 22, 2021, press release were false or materially misleading in their own right. The two patent numbers identified appear to be related to legacy Intrusion technology, not Shield. Intrusion's claims regarding the capabilities of Shield's artificial intelligence were misleading. A former employee with "close, hands-on experience" called Shield's artificial intelligence "completely faulty in every aspect," noting that the lack of investment in research and development of the software was "laughable." [23] Intrusion's claims regarding "high-speed packet capture; connection reassembly; traffic decoding and analysis; patented packet file system; patented accumulators for performance; and kill logic" were likewise misleading, as former employees who worked on Shield report that Shield's technology does not even perform full packet inspection—meaning, it doesn't actually evaluate the data and header of a packet as it passes through an inspection point, where it would normally weed out viruses, intrusions or other problematic code.[24] Rather, where the Shield program doesn't match the packet addressing information to a

[23] FE #5
[24] FE #1

known source, it simply assumes the traffic is from a bad actor and blocks the request—effectively shutting down any open network, in what is called a "fail closed" system. [25] Shield did not, in fact, "leverage" TraceCop to "train Shield's AI engine", because, as discussed above, Shield did not offer any AI capable of being "trained." Rather, it operated as a simple packet-filter firewall comparing incoming and outgoing packets to existing databases of known safe and malicious traffic. Secondly, Shield was not "in the early stage of its customer rollout" with Kimberly-Clark and/or Lippert Components, because, as discussed in depth above, neither of these companies had actually been signed to "multi-year agreements" as Shield customers. These purported contracts were a fabrication intended to drive market interest Intrusion and Shield and lacked economic substance. The claim that Shield operated as a "Network Defense and Response (NDR) product designed to kill malicious connections" rather than simply generate "alerts about suspicious traffic" was likewise false and misleading, as Shield operated—to the extent that it did—only as a packet firewall, and Intrusion knew at the time that Shield was so poorly developed that it could, in fact, ***only*** operate on an open network in "observation mode", providing "alerts about suspicious traffic" rather than "kill[ing]" it. Finally, Intrusion's claim that it possessed the "required certifications to ship Shield to every jurisdiction where it is being sold" was flagrantly false. Former employees who held senior roles in sales, with specific responsibilities for government and defense contracting, confirm that Intrusion lacked the necessary certifications required to sell its cybersecurity products to government agencies, and was marketing Shield internationally in disregard of export restrictions related to Intrusion's legacy Department of Defense contracts.[26]

84. Intrusion's misleading rebuttal of the White Diamond report appears to have been successful in temporarily staunching the bleeding, as the price of the Company's shares stabilized and rose slightly between April 21 and April 26, 2021, restoring and prolonging artificial inflation in

[25] FE #1
[26] FE #1, FE #2

the price of Intrusion's securities.

85. In its May 4, 2021, earnings call for the first quarter of fiscal 2021 (the "1Q21 Earnings Call"), management continued to set positive expectations for the rollout of Shield, attributing increased operating expenses to an "employee headcount increase" with "the additional hiring we've had to expand our sales and leadership team combined with increased marketing focus on the development and launch of Shield." Management stated that they had brought on 26 new employees in marketing and sales, eight in research and development, four in general and administrative roles, and had also increased use of outside consultants in both research and development and legacy business. Defendant Blount claimed the Company had seen "an actual unprecedented interest in a very short period of time in the Shield product" and had "struck a number of contracts, most of those being three-year contracts with some significant companies, two of those for example [being] Kimberly Clark… and [Lippert Components, Inc.]", which he went on to note were "a Fortune 500 business… [and] Fortune 2000 business", respectively. Blount stated that Kimberly Clark and Lippert had "signed international agreements for three years to be able to use the Shield product in all their international locations." Blount continued that Intrusion had "licensed over 50,000 seats to date with these companies… it's an extraordinary success I think in a very short period of time…" Blount also commented on the Company's artificial intelligence capabilities, stating that "Shield has the advantage of using the TraceCop database that we've had for 25 years, that's the largest, the most unique in the world to train our [artificial intelligence]. So, therefore, our AI can be dramatically more enhanced and more significant." In response to questions from analyst Zach Cummins of B. Riley Securities, Defendant Byrd admitted that "virtually the majority" of reported revenues for the quarter were attributable to legacy products, rather than Shield. In response to a follow-up question regarding "the number of Shield seats that you have right now," Blount reiterated that "the 50,000 seats [are] under contract for Shield but they—because of the SaaS

license, they only pay revenue online in a quarter… [so] as they ramp up and implement across the market, then you'll see more and more of the seats." When asked about plans for headcount going forward, Blount represented that "our headcount is largely stable right now."

86. Defendant Blount's statements in the May 4, 2021 earnings call were false and misleading in many of the same ways, and for the same reasons, discussed above. As previously discussed, the Company had not actually signed Kimberly-Clark and/or Lippert to "license[] over 50,000 seats to date" for Shield. Intrusion did not have "50,000 seats…under contract" with these companies, and the absence of revenue in the then-current quarter was not, as Blount represented, simply a matter of time due to "ramp up" as the Shield solution was implemented. Finally, Blount's statements about increasing headcount and expectations of stability on headcount on a going-forward basis were misleading in themselves, as they reinforced the false impression that sales and market adoption of Shield were proceeding apace, when in fact, there had been no significant contracts for sales of the Shield product and Intrusion had ample reason to know that reductions in force would be required soon.

87. On July 20, 2021, Intrusion issued a press release announcing preliminary revenue figures for the second quarter, along with "strategic actions" and "organizational changes." While the Company reiterated that "recent global interest and recognition of the Shield solution [was] increasing…" it stated that Intrusion had experienced "slower-than-anticipated sales ramp due to longer customer evaluation cycles typically seen in most enterprise security sales organizations." The Company continued to assert that, "based on customer feedback, the Company remains confident in Shield's efficacy and the valuable protection it offers…" and continued to "work closely with partners and the sales channel to further ramp testing with potential customers and convert a growing pipeline of customer engagements into recurring subscriptions." The July 20, 2021 press release also revealed that Defendant Blount had "left the company effective immediately and no longer [had] any

affiliation with Intrusion."

88. On this news, the Company's share price fell $4.24, or nearly 50%, to close a $4.26 per share on July 20, 2021, on unusually heavy trading volume.

89. On July 23, 2021, the Company filed a Form 8-K which revealed that Intrusion had "terminated the services of Jack B. Blount as the Company's President and Chief Executive Officer" on July 19, 2021.

90. The Company's share price fell another $0.75, approximately 19%, over the next two trading days, closing at $3.38 at close of the market on July 26, 2021.

91. On August 9, 2021, Intrusion filed a form 8-K with an Item 5.02 disclosure informing the market that Defendant Blount "resigned his position on the Board of Directors" and had signed a severance agreement. It also revealed that the Board had appointed Anthony J. LeVecchio, then serving as Intrusion's Executive Chairman of the Board of Directors, as interim "Principal Executive Officer".

92. On August 12, 2021, Intrusion reported its results for the second quarter of fiscal year 2021 and hosted its planned earnings call for the quarter (the "2Q21 Earnings Call"). Anthony LeVecchio, Intrusion's Chairman of the Board, led the call, along with Defendants Byrd, Davis, and Head. Defendant Head reiterated many of the Company's previous statements about the capabilities of Shield, emphasizing: "The point I want to make unmistakably clear is Shield works. It's simply a matter of ramping up…" Head continued, "… there are no showstoppers or reasons to hold back. Shield was good when we launched it and is far superior with the July 2021 release." When asked about the proportion or revenues being derived from Shield subscriptions, Defendant Byrd demurred, stating "I now know our policy is not to really talk about what's in the customer contracts, and we're not going to do so here." When asked about Intrusion's previously stated backlog of 50,000 seats pending implementation of Shield, Defendant Head waffled, saying that "I think our idea is to get

that stuff in a less fuzzy state and then give… some periodic updates…"

93. Defendants' statements on the August 12, 2021 call, that "[t] he point I want to make unmistakably clear is Shield works. It's simply a matter of ramping up…", that there were "no showstoppers or reasons to hold back", and that "Shield was good when we launched it and is far superior with the July 2021 release" were all knowingly false and misleading when made. As thoroughly discussed above, Defendant Head knew full well that (1) Shield's purported artificial intelligence solution did not work and could not be made to work in the way Intrusion suggested; (2) Intrusion had falsely represented that Shield was able to analyze threats in real-time and prevent novel cyberattacks, including specifically "zero-day" attacks; (3) Intrusion had falsely claimed to have secured contracts with Kimberly-Clark, Lippert Components, and others for 50,000 or more seats to be covered by Shield; (4) Defendants falsified its purported internal testing of the Shield solution by using fake test bed data; (5) Defendants generated artificial appearance of demand for Shield by shipping units for free; (6) Shield products were catastrophically failing in early customer rollout, including shutting down networks due to being shipped in "fail closed" configuration and numerous, "cascading" bugs and software failures; (7) Shield products were failing so pervasively in early customer rollout that customers were running the devices in "observation" mode; and (8) Shield products were generating so many error reports that Intrusion's engineering and customer support staff simply turned off alerts, while concealing functional failures from Intrusion sales personnel, and therefore from potential customers. That Defendants Head and Byrd evaded directly answering questions regarding the previously claimed "50,000 seats pending implementation" of Shield demonstrates their knowledge that the previous representations were false, and yet they failed to correct of qualify the previous misstatements despite being given multiple opportunities.

94. On August 13, 2021, Intrusion filed its Form 10-Q report for the quarterly period ended June 30, 2021 (the "2Q21 10-Q"). The 2Q21 10-Q noted that Intrusion had "executed a

planned reduction in force resulting in the termination of 20% of its employees across the organization." The Company also stated that, "Management has evaluated subsequent events through August 13, 2021… [n]o events or transactions other than those already described… have occurred subsequent to the balance sheet date that might require recognition or disclosure…"

95. On August 26, 2021, the Company filed a form 8-K Item 8.01 disclosure informing the market for the first time that on August 8, 2021, the Company received a notification from the SEC Division of Enforcement that it was conducting an investigation captioned, *In the Matter of Intrusion, Inc.* The August 26, 2021, form 8-K did not address why the SEC investigation had not been disclosed as a subsequent event in the Company's prior August 13, 2021, 10-Q or in the August 9, 2021 form 8-K.

96. That day, the Company's share price fell another $0.41, closing at $4.35, a decline of approximately 8.6%.

Defendants Falsified Testing Results, Manufactured False Sales and Inventory, and Concealed Mounting Evidence that the Shield Technology Did Not Work

97. The reality on the ground during the Class Period was that Intrusion had never actually developed the artificial intelligence capabilities the Company claimed. Former employees of the Company intimated that while Intrusion TraceCop and Savant—the legacy products which Shield purported to build upon—had real capabilities, the Company never developed a working artificial intelligence solution, and therefore, the implementation of Shield failed horribly, and the product did not work.[27]

98. For example, Intrusion's press release on February 25, 2021, stated—attributing the quote to Defendant Blount—that "Shield is the first platform that uses real-time artificial intelligence to not just block intruders, but to kill cyberattacks including zero-days…" According to a former Intrusion cyber security specialist who worked on Shield during the Class Period and

[27] FE #1, FE #5

had "close, hands-on experience" with the product, Intrusion's claim that Shield's technology could prevent "zero-day" attacks was simply "not based in reality." [28] Rather, Intrusion based this claim upon a single fluke incident during customer testing, in which Intrusion's TraceCop database identified a line of malicious code that happened to have been used previously in a different attack.[29] Intrusion's software never had the capacity to identify or prevent the truly novel exploits that define "zero day" attacks. In fact, Shield's AI was "completely faulty in every aspect," save for a limited ability to capture one specific stream of packets faster than available open-source code.[30]"Zero-day attacks – in reality – are unpreventable. All you can do is strengthen your systems and make sure your software is up-to-date."[31]

99. The Company's statement in its January 13, 2021, press release that Shield had stopped "a total of 77,539,801 cyberthreats" was also false and without any basis in reality. According to one former employee, these were simply "imaginary numbers made up by the marketing team" at Intrusion.[32]

100. Defendant Head and his team were principally responsible for programming and testing Shield, and Head knowingly misled investors by telling them repeatedly that Shield did work, had worked since it was introduced, and was improving.[33] In reality, Head knew that Shield had never worked as advertised.[34] Head told investors and potential customers that Shield had general release availability, when in fact he knew full well that the Company's testing process was fraudulent, and Intrusion was essentially beta-testing the product on live users while ostensibly attempting to address hundreds of known and ongoing software issues.[35] Defendant

[28] FE #5
[29] FE #5
[30] FE #5
[31] FE #5
[32] FE #5
[33] FE #2
[34] FE #2
[35] FE #2

Head and Intrusion's engineering team were not using real data for the Company's initial test bed.[36]

101. At Head's direction, Intrusion's Customer Service Department ignored warnings and alarms from customers who had problems with the Shield equipment, essentially turning off alerts and failing to address the reported issues.[37]

102. Intrusion began aggressively hiring staff, particularly in sales and marketing, to push the Shield product as quickly as possible, in hopes of capitalizing on the Company's false claims about Shield's capabilities before the truth about Shield became known. According to confidential informants, marketing teams understood that because they were "selling an illusion, then [they had to] hurry up and build [that] illusion." [38] Former Intrusion personnel noted that while there were warning signs of problems with the Shield product, the actual issues were concealed from the sales team.[39]

103. To generate interest in Shield, Company insiders—led by Defendant Head—manipulated Company accounting by diverting sales from legacy contracts to generate the appearance of revenue from sales of Shield, where none existed.[40] They also generated false inventory levels and shipments of Shield devices.[41] Finally, Defendant Head—with the knowing assistance of the Defendant Davis—suppressed evidence and customer reports that Shield was not working and retaliated against internal whistleblowers by firing them.[42]

104. Intrusion sought to demonstrate success in marketing Shield by issuing a press release on March 31, 2021, representing to the market that they had signed global consumer products company Kimberly-Clark as a Shield customer. Shortly thereafter, on April 6, 2021, the

[36] FE #3
[37] FE #2
[38] FE #5
[39] FE #2
[40] FE #1, FE #4
[41] FE #3
[42] FE #2

Company issued another press release that it had signed Lippert up for Shield as well. On its May 4, 2021, earnings call, Defendant Blount trumpeted these contracts, claiming that Shield had already secured sales of 50,000 seats between the two. Both Kimberly-Clark and Lippert were existing customers of Intrusion's legacy services, and never paid for the Shield product. Instead, Defendants conspired to fraudulently book billings on other business lines to Kimberly-Clark and Lippert during the period as revenues from sales of Shield.[43] Kimberly-Clark's existing Z-Scaler infrastructure was not even compatible with Shield.[44] Neither Kimberly-Clark nor Lippert received or used and Shield units.[45] Defendant Blount and a cyber defense officer at Kimberly-Clark conspired to allow Intrusion to report that Kimberly-Clark has signed on as a Shield customer and received equipment, when in fact they had not.[46] When one former employee challenged Defendant Head on false statements about the number of Shield installations the Company had in place, head "hemmed and hawed", claiming that Kimberly-Clark had merely delayed its installation of Shield because it had recently appointed a new Chief Information Security Officer.[47] "But the truth is there was no revenue. It was a lie to cover up" the truth.[48] Said another former Intrusion employee, "The Company would say they made sales of Shield in certain areas, but those were not really sales of Shield—that's fraud… They'd say they were bringing in money from certain places, but they were not" [49] "It was really a sale of their legacy stuff, and Intrusion said, 'Can we just call this a Shield sale for $6 million?' They didn't care."[50] Intrusion's press release trumpeting an endorsement of Shield from an officer at Kimberly-Clark was likewise fraudulent: "How could Kimberly-Clark give an endorsement of a product when

[43] FE #1
[44] FE #1
[45] FE #4
[46] FE #4
[47] FE #4
[48] FE #4
[49] FE #1
[50] FE #1

they never had it?"[51]

105. Defendant Head and others within Intrusion also sought to generate Shield sales by violating export controls to sell Shield equipment internationally. In or about August 2021, Defendant Head travelled to Mexico on a sales campaign and reported back that several Mexican companies were interested in purchasing equipment.[52] After FE #1, Intrusion's Vice President of Sales for Government and Defense, told Head that as a cleared defense contractor, Intrusion didn't have permission to sell or export the equipment in Mexico, Head decided to ship the equipment anyway.[53] Because of the export control issues, Intrusion's distributor refused to ship the equipment, so instead, Defendant Head transferred the account to another sales team and attempted to recruit an Intrusion sales representative to "smuggle" the equipment to Mexico in his personal luggage.[54] A confidential witness informed the sales representative that doing so might be a felony, and the representative ultimately refused.[55]

106. Defendant Head and others also manipulated Intrusion's reported inventory to create the false appearance that Shield units were being shipped to customers. Former employees report that there was questionable inventory of the Company's Shield devices, and an inventory audit revealed conflicts with the records kept by Defendant Head.[56]

107. Internally, Intrusion's sales personnel were growing increasingly suspicious. "We were trying to figure out as employees how in the world did they get contracts for something that doesn't exist." [57] "We had heard internally of violations of contracts and other things going on internally – contracting that was outside the scope."[58]

---

[51] FE #4
[52] FE #2
[53] FE #1, FE #2
[54] FE #2
[55] FE #2
[56] FE #3
[57] FE #4
[58] FE #4

108. Former employees reported that "something happened in January [2021]—the solution [Shield] was failing and shutting down computer networks." [59] "For whatever reason, the hardware was set up to fail close—and hardware hasn't been set up to fail close since the 1990s."[60] The sales team later learned that customers who had received the Shield equipment were not setting it into an active mode to intercept nefarious traffic — because that was not working.[61] Rather it was only being used in "observation" mode, because the equipment was shutting down networks, and in at least one case even shutting down a customer's network while in this "observation" mode.[62]

109. Around late June and early July of 2021, two confidential witnesses decided they had to figure out what was really going on and started inquiring with personnel in other Intrusion departments.[63] They learned that "everything [Intrusion] had sold and set up to that point was failing miserably, left and right… [The Company] had customers saying, 'Come pick this up, we're not dealing with this.'"[64] But Intrusion's management team offered no solutions, suggesting instead that the sales team give the equipment away for free in order to preserve the illusion that the product was working in the field.[65] The witnesses soon learned from Intrusion's Vice President of Customer Support that Shield equipment was failing to the point that it was setting off notification alarms within the Customer Support unit, which Intrusion simply ignored, turning off the alarms and never informing the sales team.[66] In late August of 2021, Intrusion's VP of Engineering Blake Dumas admitted to two former employees that, "You see [Shield] is

[59] FE #2
[60] FE #2
[61] FE #2
[62] FE #2
[63] FE #2, FE #1
[64] FE #2
[65] FE #2
[66] FE #2

throwing so many alarms at customer service that they're shutting off alerts." [67] Then the witnesses inquired to Dumas just how buggy the Shield devices were, Dumas reported that the customer service and engineering teams were finding approximately "1,000 [bugs] a month, and then when they fix those, more come up… It's cascading."[68]

110. One of those former employees received confirmation from Intrusion's engineering team that Shield was not ready for general availability release, contrary to the Company's previous claims, and was fired after bringing the issue to the attention of the executive team.[69] The other was fired after repeatedly discussing concerns with Defendant Davis.[70] The reports from former Intrusion employees are ruinous. "This thing [Shield] didn't work. It never worked. There's nothing here. [Intrusion's leadership] are committing fraud and they don't seem to care."[71]

111. Witnesses also told Plaintiff's counsel that Defendant Blount was ultimately fired because he was going to expose the fraud within the Company.[72]

112. A former senior member of Defendant Blount's staff reports that in May or June or 2021—notably, after the White Diamond report was issued and this lawsuit was commenced in April of 2021—Blount and his team became suspicious that there was "something going on" with Intrusion's internal practices with respect to the Shield product, particularly with respect to Defendant Head's team.[73] "There was so much lying going on here…"[74] The witness stated that it was their belief that, "any statements that Blount made that were inaccurate or dubious were based on information fed to him by the engineering team, and that he was misled… [Blount]

[67] FE #1, FE #2
[68] FE #2
[69] FE #1, FE #2
[70] FE #2
[71] FE #2
[72] FE #4, FE #3
[73] FE #3
[74] FE #3

would go to the marketing team, the engineering team before he took any numbers public. He's ultimately responsible, but how would he know?"[75] Blount began to discover some of the shady business practices of Defendant Head and his team.[76] Blount's team learned that Intrusion's engineering team hadn't been using a real test bed to generate testing results on the Shield product.[77] In addition, they learned that sales of Shield products were booked, and shipments recorded, but the machines were never turned on.[78] They also found evidence of numerous Shield units which were recorded as being in inventory, but did not actually exist.[79] Approximately a week before Blount was fired, he ordered Intrusion's Director of Operations, Denise Beckman, to conduct an internal inventory audit of Shield equipment.[80] It was then that Defendant Head "got really interested."[81] Beckman "came back three times and said, 'I can't match [Head's] numbers.'"[82] Defendant Blount was subsequently and summarily dismissed by Intrusion's Board of Directors. It was six weeks from the time [Blount's team] started talking about it that [Blount] got fired."[83] The witness reports that Defendant Head and his team were being dishonest with Blount and other members of senior management: "I thought I understood what we were doing—but I [now] think engineering was lying and not coming clean about things."[84]

CLASS ACTION ALLEGATIONS

113. Plaintiff brings this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3) on behalf of a class, consisting of all persons and entities that

[75] FE #3
[76] FE #3
[77] FE #3
[78] FE #3
[79] FE #3.
[80] FE #3
[81] FE #3
[82] FE #3
[83] FE #3
[84] FE #3

purchased Intrusion securities between October 14, 2020, and August 26, 2021, inclusive, and who were damaged thereby (the "Class"). Excluded from the Class are Defendants, the officers and directors of the Company, at all relevant times, members of their immediate families and their legal representatives, heirs, successors, or assigns, and any entity in which Defendants have or had a controlling interest.

114. The members of the Class are so numerous that joinder of all members is impracticable. Throughout the Class Period, Intrusion's shares actively traded on the NASDAQ. While the exact number of Class members is unknown to Plaintiff at this time and can only be ascertained through appropriate discovery, Plaintiff believes that there are at least hundreds or thousands of members in the proposed Class. Millions of Intrusion shares were traded publicly during the Class Period on the NASDAQ. Record owners and other members of the Class may be identified from records maintained by Intrusion or its transfer agent and may be notified of the pendency of this action by mail, using the form of notice similar to that customarily used in securities class actions.

115. Plaintiff's claims are typical of the claims of the members of the Class as all members of the Class are similarly affected by Defendants' wrongful conduct in violation of federal law that is complained of herein.

116. Plaintiff will fairly and adequately protect the interests of the members of the Class and has retained counsel competent and experienced in class and securities litigation.

117. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual members of the Class. Among the questions of law and fact common to the Class are:

(a) whether the federal securities laws were violated by Defendants' acts as alleged herein;

(b) whether statements made by Defendants to the investing public during the Class Period omitted and/or misrepresented material facts about the business, operations, and prospects of Intrusion; and

(c) to what extent the members of the Class have sustained damages and the proper measure of damages.

118. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy since joinder of all members is impracticable. Furthermore, as the damages suffered by individual Class members may be relatively small, the expense and burden of individual litigation makes it impossible for members of the Class to individually redress the wrongs done to them. There will be no difficulty in the management of this action as a class action.

ADDITITIONAL ALLEGATIONS SUPPORTING FALSITY AND SCIENTER ALLEGATIONS

119. Defendant Head, as a co-founder of the Company and its Chief Technology Officer, actively perpetuated the fraud by lying about Shield's capabilities and state of development both internally to intrusion and externally to investors. Head attended and actively participated in Intrusion's quarterly earnings calls and other investor calls, in which he personally lied to the market and supported or acquiesced in material misrepresentations by other members of the Company's senior management. Former employees confirm that Head was principally and directly responsible for the development and internal testing of Shield, and knew full well that the Shield AI wasn't working, that the Company's internal testing procedures—which he designed and supervised himself—were fraudulent and unreliable, and that his and the Company's representations that Kimberly-Clark and Lippert Components had contracted for thousands of Shield seats and that Kimberly-Clark was actively paying for Shield and generating revenue for the Company were entirely false. One witness said: "[t]here is no way Joe didn't know… [the witness] personally told

[Head] at least three times to his face" about the problems with Shield.[85] The witness further reported that Head was personally informed of the problems with Shield at regular intervals, and that Head himself admitted in an internal meeting that he had heard from Intrusion's head of sales that the Shield boxes were not working, and that potential customers were returning the equipment or electing not to plug the units in.[86] The same witness confronted Head personally twice during forecast calls, which also included Intrusion's head of business development.[87]

120. Defendant Blount, as CEO and Chairman during the Class Period, made numerous false and misleading statements concerning Shield to investors and the public, including in press releases, investor calls, social media, and public presentations, as detailed in the foregoing sections of this Complaint. A former employee who worked closely with and reported to Defendant Blount reported that in May or June 2021, Blount became suspicious that he and the executive team were provided incomplete or misleading information by Defendant Head and others within Intrusion, and took action to investigate, which ultimately led to his dismissal as CEO.[88] Even crediting these reports as accurate, it appears Defendant Blount did not take any reasonable action to investigate or ascertain the credibility of information provided by Defendant Head or others until May or June 2021, well after the issuance of the White Diamond report on April 13, 2021, and the initiation of this litigation on April 16, 2021. Other evidence, described herein, establishes that Defendant Blount had access to information from which he knew or should have known that the statements he made to the public regarding Intrusion Shield were false and misleading, or at least potentially false and misleading, prior to making them. Other confidential witness testimony supports the conclusion that Defendant Blount himself conspired with officers from Kimberly-Clark and/or Lippert to support the Defendants' false and misleading statements concerning the existence of contracts to provide

[85] FE #2
[86] FE #2
[87] FE #2
[88] FE #3

Intrusion Shield services for 50,000+ paid seats.[89] Other evidence, as described herein, supports the conclusion that Defendant Blount misstated his own professional history and accomplishments, and/or acquiesced in such misstatements by the Company and other agents of the Company on his behalf, including with respect to statements that he had previously served as "CIO of the U.S. Department of Agriculture."[90] Taken together, this evidence supports the conclusion that Defendant Blount knew, or at least should have known and was willfully or recklessly ignorant as to, the false and misleading character of statements made by himself, the Company, and other agents of the Company during the Class Period, as detailed herein.

121. Defendant Michael Paxton, as Intrusion's CFO until his retirement on or about December 31, 2020, was aware of, or at least had reason to believe and did in fact suspect, malfeasance within Intrusion and misstatements regarding Shield. Rather than investigate or challenge the false and misleading statements of Head, Blount, and others, Paxton acquiesced in their misrepresentations and quietly retired from his position as CFO, while simultaneously planning to sell and transfer millions of dollars of Intrusion stock prior to the revelation of the Company's misstatements beginning with the White Diamond report in April 2021. Defendant Paxton transferred 490,000 shares of Intrusion common stock from a trust in his control to his adult children, as reported to the SEC on Forms 4 dated March 13 and March 16, 2021. He further sold 52,500 shares of Intrusion common stock in open market transactions between March 12 and April 8, 2021, during a time of historic high prices of between $24.80 and $27.50 per share, pursuant to a Form 144 file March 12, 2021. According to the same report, Paxton acquired these securities in open-market transactions on November 15-17, 2006. The split-adjusted price per share of Intrusion stock on those dates was between $0.39 and $0.47 per share, implying an investment gain to Defendant Paxton of approximately $1.3 million. The market value of shares transferred from Defendant Paxton's trust to

[89] FE #4
[90] See, ¶¶ 39-41, supra.

his adult children in the same period exceeded $120 million. Defendant Paxton's trade do not appear to have been made pursuant to any pre-existing Rule 10b5-1 plan. Rather, it appears Defendant Paxton elected to cash out as much of his stock as possible while the price of Intrusion's stock remained artificially inflated by Defendants' fraud. Defendant Paxton's providentially timed exit and disposition of millions of dollars of Intrusion stock almost immediately before the truth was revealed and its price collapsed demonstrate Paxton's scienter.

122. Defendant Franklin Byrd, as the Company's successor CFO, jointed the Company or about December 1, 2020. A former employee and confidential witness who was present on investor calls with Byrd, said that Intrusion's statements in those calls, specifically regarding contracts for the sale of Shield to Kimberly-Clark and Lippert, were likely known to Byrd to be false or without any reliable basis. "it was information that Franklin knew to be false—or a very grey area—and he let them go ahead."[91] When, during an investor call on August 12, 2021, an analyst asked for specifics "the average roughly price being paid" per head by Shield customers, Defendant Byrd declined to answer, responding that: "…our policy is not to really talk about what's in the customer contracts, and we're not going to do so here." The same former employee cited this as an example of Defendant Byrd's complicity in Intrusion's misleading statements.

123. Defendant Davis, the Company's CMO, was specifically informed about serious and continuing problems with Intrusion Shield and elected to retaliate by firing whistleblowers rather than correct the Company's false and misleading statements about the product. One former employee, who reported directly to Defendant Davis, confirmed: "I went [Davis] several times and said 'You can't say this' and I was told to shut up and go away."[92] A different former employee subsequently had a conversation with Defendant Davis, in which he told Davis: "… You understand someone is going to take the fall for this. This doesn't go unnoticed. There's an SEC investigation. A

[91] FE #4
[92] FE #4

class action lawsuit. And there's word that there's a [Department of Defense] investigation coming soon. You understand [Defendant Head] isn't going to take the fall for this. You will."[93] Rather than take any action to address the issues brought to his attention, Defendant Davis elected to fire the reporting employee a week later.[94] A third former employee implicated Defendant Davis as one of the parties within Intrusion who cooperated with Defendant Joe Head's attempts to conceal the Company's questionable business practices from scrutiny, noting that he, along with Head, shut down efforts to bring Intrusion into compliance and obtain necessary certifications to market Shield to U.S. government entities.[95] David and Head willfully avoided the process to obtain the necessary certifications to market Shield to U.S. government agencies. A former employee reported that "[w]hen [they] asked about sanitization procedures (to keep sensitive information secure), the engineers laughed at [them]… Joe [Head] fought tooth and nail over the certification process. He just balked at it."[96] When the former employee went to Davis and told him that Intrusion would be unable to market Shield to government entities without such certifications, Davis sided with Head, responding: "I can't do what [CTO Joe Head] is asking me to do and do the certification stuff."[97] Defendant Davis was thus clearly aware that practices within Joe Head's purview presented potential vulnerabilities to the Company if subjected to closer examination. Defendant Davis nevertheless participated in investors calls in which he made or acquiesced in false and potentially misleading statements regarding Intrusion Shield.

124. Defendant Gero was a purportedly independent Director for Intrusion throughout the Class Period. A former employee specifically identified Gero as a "bad guy" on the Board with close ties to Defendant Joe Head.[98] Defendant Gero also sits on the board (and is as a former Chairman of)

[93] FE #2
[94] FE #2
[95] FE #1
[96] FE #1
[97] FE #1
[98] FE #1

Lippert Components, Inc. and its corporate parent, LCI Industries (NYSE: LCII), and appears to have facilitated the Company's statements that it had signed Lippert as a Shield customer, which were false and misleading when made, as detailed herein.

APPLICABILITY OF PRESUMPTION OF RELIANCE
(FRAUD-ON-THE-MARKET DOCTRINE)

125. The market for Intrusion's securities was open, well-developed, and efficient at all relevant times. As a result of the materially false and/or misleading statements and/or failures to disclose, Intrusion's securities traded at artificially inflated prices during the Class Period. On April 13, 2021, the Company's share price closed at a Class Period high of $28.25 per share. Plaintiff and other members of the Class purchased or otherwise acquired the Company's securities relying upon the integrity of the market price of Intrusion's securities and market information relating to Intrusion, and have been damaged thereby.

126. During the Class Period, the artificial inflation of Intrusion's shares was caused by the material misrepresentations and/or omissions particularized in this Complaint causing the damages sustained by Plaintiff and other members of the Class. As described herein, during the Class Period, Defendants made or caused to be made a series of materially false and/or misleading statements about Intrusion's business, prospects, and operations. These material misstatements and/or omissions created an unrealistically positive assessment of Intrusion and its business, operations, and prospects, thus causing the price of the Company's securities to be artificially inflated at all relevant times, and when disclosed, negatively affected the value of the Company shares. Defendants' materially false and/or misleading statements during the Class Period resulted in Plaintiff and other members of the Class purchasing the Company's securities at such artificially inflated prices, and each of them has been damaged as a result.

127. At all relevant times, the market for Intrusion's securities was an efficient market for the following reasons, among others:

(a) Intrusion shares met the requirements for listing, and was listed and actively traded on the NASDAQ, a highly efficient and automated market;

(b) As a regulated issuer, Intrusion filed periodic public reports with the SEC and/or the NASDAQ;

(c) Intrusion regularly communicated with public investors via established market communication mechanisms, including through regular dissemination of press releases on the national circuits of major newswire services and through other wide-ranging public disclosures, such as communications with the financial press and other similar reporting services; and/or

(d) Intrusion was followed by securities analysts employed by brokerage firms who wrote reports about the Company, and these reports were distributed to the sales force and certain customers of their respective brokerage firms. Each of these reports was publicly available and entered the public marketplace.

128. As a result of the foregoing, the market for Intrusion's securities promptly digested current information regarding Intrusion from all publicly available sources and reflected such information in Intrusion's share price. Under these circumstances, all purchasers of Intrusion's securities during the Class Period suffered similar injury through their purchase of Intrusion's securities at artificially inflated prices and a presumption of reliance applies.

129. A Class-wide presumption of reliance is also appropriate in this action under the Supreme Court's holding in *Affiliated Ute Citizens of Utah v. United States*, 406 U.S. 128 (1972), because the Class's claims are, in large part, grounded on Defendants' material misstatements and/or omissions. Because this action involves Defendants' failure to disclose material adverse information regarding the Company's business operations and financial prospects—information that Defendants were obligated to disclose—positive proof of reliance is not a prerequisite to recovery. All that is necessary is that the facts withheld be material in the sense that a reasonable investor might have

considered them important in making investment decisions. Given the importance of the Class Period material misstatements and omissions set forth above, that requirement is satisfied here.

FIRST CLAIM
Violation of Section 10(b) of The Exchange Act and Rule 10b-5 Promulgated Thereunder Against All Defendants

130. Plaintiff repeats and re-alleges every allegation contained above as if fully set forth herein.

131. During the Class Period, Defendants carried out a plan, scheme and course of conduct which was intended to and, throughout the Class Period, did: (i) deceive the investing public, including Plaintiff and other Class members, as alleged herein; and (ii) cause Plaintiff and other members of the Class to purchase Intrusion's securities at artificially inflated prices. Infurtherance of this unlawful scheme, plan and course of conduct, Defendants, and each defendant, took the actions set forth herein.

132. Defendants (i) employed devices, schemes, and artifices to defraud; (ii) made untrue statements of material fact and/or omitted to state material facts necessary to make the statements not misleading; and (iii) engaged in acts, practices, and a course of business which operated as a fraud and deceit upon the purchasers of the Company's securities in an effort to maintain artificially high market prices for Intrusion's securities in violation of Section 10(b) of the Exchange Act and Rule 10b-5. All Defendants are sued either as primary participants in the wrongful and illegal conduct charged herein or as controlling persons as alleged below.

133. Defendants, individually and in concert, directly and indirectly, by the use, means or instrumentalities of interstate commerce and/or of the mails, engaged and participated in a continuous course of conduct to conceal adverse material information about Intrusion's financial well-being and prospects, as specified herein.

134. Defendants employed devices, schemes, and artifices to defraud, while in possessionof

material adverse non-public information and engaged in acts, practices, and a course of conduct as alleged herein in an effort to assure investors of Intrusion's value and performance and continued substantial growth, which included the making of, or the participation in the making of,untrue statements of material facts and/or omitting to state material facts necessary in order to make the statements made about Intrusion and its business operations and future prospects in light of the circumstances under which they were made, not misleading, as set forth more particularly herein, and engaged in transactions, practices and a course of business which operated as a fraud and deceit upon the purchasers of the Company's securities during the Class Period.

135. Each of the Individual Defendants' primary liability and controlling person liability arises from the following facts: (i) the Individual Defendants were high-level executives and/or directors at the Company during the Class Period and members of the Company's management team or had control thereof; (ii) each of these defendants, by virtue of their responsibilities and activities as a senior officer and/or director of the Company, was privy to and participated in the creation, development and reporting of the Company's internal budgets, plans, projections and/orreports; (iii) each of these defendants enjoyed significant personal contact and familiarity with theother defendants and was advised of, and had access to, other members of the Company's management team, internal reports and other data and information about the Company's finances, operations, and sales at all relevant times; and (iv) each of these defendants was aware of the Company's dissemination of information to the investing public which they knew and/or recklessly disregarded was materially false and misleading.

136. Defendants had actual knowledge of the misrepresentations and/or omissions of material facts set forth herein, or acted with reckless disregard for the truth in that they failed to ascertain and to disclose such facts, even though such facts were available to them. Such defendants' material misrepresentations and/or omissions were done knowingly or recklessly and for the purpose and effect of concealing Intrusion's financial well-being and prospects from the investing public and

supporting the artificially inflated price of its securities. As demonstrated by Defendants' overstatements and/or misstatements of the Company's business, operations, financial well-being, and prospects throughout the Class Period, Defendants, if they did not have actual knowledge of the misrepresentations and/or omissions alleged, were reckless in failing to obtain such knowledge by deliberately refraining from taking those steps necessary to discover whether those statements were false or misleading.

137. As a result of the dissemination of the materially false and/or misleading information and/or failure to disclose material facts, as set forth above, the market price of Intrusion's securities was artificially inflated during the Class Period. In ignorance of the fact that market prices of the Company's securities were artificially inflated, and relying directly or indirectly on the false and misleading statements made by Defendants, or upon the integrity of themarket in which the securities trades, and/or in the absence of material adverse information that was known to or recklessly disregarded by Defendants, but not disclosed in public statements by Defendants during the Class Period, Plaintiff and the other members of the Class acquired Intrusion's securities during the Class Period at artificially high prices and were damaged thereby.

138. At the time of said misrepresentations and/or omissions, Plaintiff and othermembers of the Class were ignorant of their falsity, and believed them to be true. Had Plaintiff and the other members of the Class and the marketplace known the truth regarding the problems that Intrusion was experiencing, which were not disclosed by Defendants, Plaintiff and other members of the Class would not have purchased or otherwise acquired their Intrusion securities, or, if they had acquired such securities during the Class Period, they would not have done so at the artificially inflated prices which they paid.

139. By virtue of the foregoing, Defendants violated Section 10(b) of the Exchange Act and Rule 10b-5 promulgated thereunder.

140. As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and the other members of the Class suffered damages in connection with their respective purchases and sales of the Company's securities during the Class Period.

SECOND CLAIM
Violation of Section 20(a) of The Exchange ActAgainst the Individual Defendants

141. Plaintiff repeats and re-alleges every allegation contained above as if fully set forth herein.

142. Individual Defendants acted as controlling persons of Intrusion within the meaningof Section 20(a) of the Exchange Act as alleged herein. By virtue of their high-level positions andtheir ownership and contractual rights, participation in, and/or awareness of the Company's operations and intimate knowledge of the false financial statements filed by the Company with the SEC and disseminated to the investing public, Individual Defendants had the power to influence and control and did influence and control, directly or indirectly, the decision-making of the Company, including the content and dissemination of the various statements which Plaintiff contends are false and misleading. Individual Defendants were provided with or had unlimited access to copies of the Company's reports, press releases, public filings, and other statements alleged by Plaintiff to be misleading prior to and/or shortly after these statements were issued and had the ability to prevent the issuance of the statements or cause the statements to be corrected.

143. Individual Defendants had direct and supervisory involvement in the day-to-day operations of the Company and, therefore, had the power to control or influence the particular transactions giving rise to the securities violations as alleged herein, and exercised the same.

144. As set forth above, Intrusion and Individual Defendants each violated Section 10(b) and Rule 10b-5 by their acts and omissions as alleged in this Complaint. By virtue of their position as controlling persons, Individual Defendants are liable pursuant to Section 20(a) of the Exchange Act.

As a direct and proximate result of Defendants' wrongful conduct, Plaintiff and other members of the Class suffered damages in connection with their purchases of the Company's securities during the Class Period.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff pray for relief and judgment, as follows:

(a) Determining that this action is a proper class action under Rule 23 of the Federal Rules of Civil Procedure;

(b) Awarding compensatory damages in favor of Plaintiff and the other Class members against all defendants, jointly and severally, for all damages sustained because of Defendants' wrongdoing, in an amount to be proven at trial, including interest thereon;

(c) Awarding Plaintiff and the Class their reasonable costs and expenses incurred in this action, including counsel fees and expert fees; and

(d) Such other and further relief as the Court may deem just and proper.

JURY TRIAL DEMANDED

Plaintiff hereby demands a trial by jury.

Dated: February 7, 2022

Respectfully submitted,

STECKLER WAYNE COCHRAN CHERRY, PLLC

/s/ Stuart L. Cochran
Stuart L. Cochran
Texas Bar No.: 24027936
Braden M. Wayne
Texas Bar No.: 24075247
12720 Hillcrest Rd., Suite 1045
Dallas, Texas 75230
T: 972-387-4040
F: 972-387-4041
stuart@swclaw.com
braden@swclaw.com

Liaison Counsel for Lead Plaintiff and the Proposed Class

THE ROSEN LAW FIRM, P.A.
Laurence M. Rosen (*pro hac vice* to be filed)
Phillip Kim (*pro hac vice*)
Brent J. LaPointe (*pro hac vice*)
275 Madison Avenue, 40th Floor
New York, NY 10116
Phone: (212) 686-1060
Fax: (212) 202-3827
Email: lrosen@rosenlegal.com
Email: pkim@rosenlegal.com
Email: blapointe@rosenlegal.com

Counsel for Lead Plaintiff and the Proposed Class

CERTIFICATE OF SERVICE

I hereby certify that on February 7, 2022, I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which electronically delivered a copy of the same to all counsel of record.

/s/ Stuart L. Cochran
Stuart L. Cochran